Webex Control Hub

(コンプライアンス) データシート

目次

コンプライアンスの概要

企業は、従業員がコラボレーション ツールを使用して偶発的に、または悪意を持って機密情報や重要な情報を送信しないように制御する必要があります。このような情報の例には、合併および買収情報、クレジットカード番号、ソーシャルセキュリティ番号、知的財産、診療録などが挙げられます。Webex は、そのオープン API エコシステムを介して、データセキュリティと完全性を保証するためいくつかのデータ損失防止（DLP）およびアーカイブソリューションを統合しました。侵害の影響は深刻になる場合があるため、Webex は パートナー統合を介して Control Hub の可視性と制御を導入し、お客様がコンプライアンスポリシーの遵守を管理できるようにしました。Control Hub は、Webex サービスのプロビジョニングと管理を直感的に行うことができる Web ベースの一元管理ポータルです。

Pro Pack for Control Hub は、既存のコンプライアンス、セキュリティ、および分析ソフトウェアと連携してより高度な機能ときめ細かい制御を必要とするお客様向けのオプションです。

法的な理由で従業員が生成したコンテンツを検索・抽出する必要がある場合、e-discovery 検索・抽出機能を使用すると、コンプライアンス管理者はこの情報をレポートで抽出できます。

また、企業はビジネス価値のないデータを定期的かつ自動的に消去して、セキュリティリスクを制御し、責任を抑えたいとも考えています。保持機能は、お客様のニーズに応じてこのメカニズムを構成する機能を提供します。

さらに、コンプライアンス責任者は保持ポリシーに例外を追加し、ユーザが調査対象になっている間はそのユーザを訴訟ホールドにすることができます。これにより、調査中に組織全体の保持ポリシーによってユーザーが自身のコンテンツを保持し、削除できないようにします。

また、Webex は、Webex の既存ネイティブファイル共有とストレージに加えて、IT 管理者がユーザーに対して Microsoft OneDrive、SharePoint Online、および Box をエンタープライズコンテンツ管理（ECM）ソリューションとして有効にできる柔軟性も備えています。ユーザーは、Webex Spaces で、OneDrive、SharePoint Online、Box の最新ファイルを共有、編集、取得できる一方で、ファイルは、安全に保管され、お客様の既存 DLP/CASB およびマルウェア対策ソリューションを通じて保護されます。

Webex スペースの所有権

Webex は、組織の境界を越えたコラボレーションをサポートし、促進します。そのため、ユーザは他の企業の社員と通信することができます。他の企業の社員が存在するスペースは、組織が混合したスペースとなります。コンプライアンス アサーションの理由から、組織が混合したスペースを含むすべてのスペースは常に特定の組織に帰属します。このために、Webex にはスペースの所有権という概念が存在します。所有権の持ち方はグループスペースと 1 対 1 スペースで（ダイレクトスペース）で異なります。

Webex グループスペース

グループ スペースの場合、単一の組織がそのスペースの所有者です。ユーザがスペースを作成する組織がスペースの所有者となります。スペースを所有する組織には、特定の権限があります。組織に、その組織が所有していないグループスペースの参加者であるユーザーがいる場合、その組織を参加組織と言います。

表 1 に、コンプライアンス責任者のコンテンツ権限の概要を示します。

表 1. グループ スペースに対するコンプライアンス責任者のコンテンツ権限

権限	所有組織	参加組織
CREATE		
スペースにコンテンツを投稿	はい	はい
READ		
自身の組織のユーザがスペースに投稿したコンテンツ（メッセージとファイル）の読み取り	はい	はい
スペース内の任意のユーザが投稿したコンテンツの読み取り	はい	×
UPDATE		
ユーザがスペースに投稿したコンテンツを変更する	×	×
DELETE		
スペースの保持ポリシーを定義	はい	×
任意のユーザがスペースに投稿したコンテンツを削除する	はい	×
自身の組織のユーザによって投稿されたスペース内のコンテンツを削除する	はい	はい

2 つの異なる組織間のユーザ同士の 1 対 1 (ダイレクト) スペースは、2 つの組織間で共有所有権を提供します。表 2 に、スペースのコンテンツ権限に関する 1 対 1 のスペース（個人間の通信）での各参加組織の権限の概要を示します。

どちらの組織も、独立した保持ポリシーを設定できます。1 つの組織の保持ポリシーが期限切れになると、そのユーザによって送信されたメッセージが削除されます。2 つ目の組織の保持ポリシーが期限切れになると、そのユーザによって送信されたメッセージが削除されます。

表 2.　　1 対 1 のスペースに対するコンプライアンス責任者のコンテンツ権限（個人間の通信）

権限	各参加組織
CREATE	
スペースにコンテンツを投稿	×
READ	
自身の組織のユーザがスペースに投稿したコンテンツ（メッセージとファイル）の読み取り	はい
スペース内の任意のユーザが投稿したコンテンツの読み取り	はい
UPDATE	
ユーザがスペースに投稿したコンテンツを変更する	いいえ
DELETE	
スペースの保持ポリシーを定義	はい
任意のユーザがスペースに投稿したコンテンツを削除する	いいえ
自身の組織のユーザによって投稿されたスペース内のコンテンツを削除する	はい

Events API

イベント API は、コンプライアンス担当者がアクセスできる REST エンドポイントです。これは SEM システムと同様に、Webex アプリでの多くのユーザーアクションの証跡をイベントログとして提供し、多くの DLP/CASB パートナーへ統合する際に使用することで、ユーザーの行動を把握して損害や損失を軽減します。

Webex では、ユーザーは、自社が所有するスペースに招待したり別の会社のスペースに参加したりして、社外の人とコミュニケーションを取ることができます。Events API は、監視組織が所有していないスペースであっても、ユーザのアクティビティを可視化します。Events API を使用することで、そのようなコンテンツの問題を是正するためのアクションを DLP ソフトウェアで実行することもできます。 https://developer.webex.com/resource-events.html。

Webex Meetings を使用すると、ユーザーは自身が主催する会議のゲストとして組織内外の参加者を招待できます。共通アイデンティティ（CI）にリンクされ有効になっているサイトの場合、ホスト組織のコンプライアンス責任者は、Webex Events API を通じて、会議イベント、録音、トランスクリプトにアクセスできます。会議関連のデータ（およびメタデータ）には、会議を主催する組織のコンプライアンスオフィサーのみがアクセスできます。

eDiscovery：検索および抽出

コンプライアンスオフィサーは法的調査の際、必要に応じて Web からアクセス可能な eDiscovery 検索・抽出コンソールを使用して、組織でユーザーが作成したデータをオンデマンドで抽出できます。データの検索は、既存のユーザと削除されたユーザの両方の電子メール アドレス（最大 500 個）と、スペース ID（最大 5 個）を使用して実行できます。また、このインターフェイスを使用して、コンプライアンス責任者はレポートの時間枠を指定することもできます。

検索レポートは、すべてのアクティビティをスペース別に整理した EML 形式の zip ファイルとしてダウンロードできます。オプションで、EML 形式の出力ファイルをダウンストリームの eDiscovery ツールに取り込み、データに対してさらにクエリや後処理を実行できます。コンプライアンス責任者は、ダウンロードを開始して完了するために、ダウンロードマネージャ（クロスプラットフォームダウンロードツール）をラップトップまたはサーバにダウンロードしてインストールする必要があります。オプションで、レポートのダウンロードから添付ファイルを除外し、ユーザが生成したメッセージのみを検査することができます。これにより、時間とネットワーク帯域幅を節約し、特定のユーザまたは関心のあるスペースに対する将来の反復検索を容易にします。検索レポートには、コンプライアンス責任者の組織内のユーザが主催する会議用に生成されたトランスクリプトも含まれます。コンプライアンス責任者は、Webex Messaging および Webex Meetings のコンテンツを eDiscovery レポートに含めることができます。

この機能へのアクセスは、ロールベースのアクセス コントロール内にある、組織によって定義されたコンプライアンス責任者に制限されます。eDiscovery 検索とレポートは、Control Hub からアクセスできます。レポートサマリーには、ユーザー数、アクティブ、ファイル、ホワイトボード数、スペース ID、会議、録音情報やその他メタデータなどの情報が表示されます。

コンプライアンス責任者は、過去のレポートのリストを表示し、EML 形式でダウンロードしてから、選択した eDiscovery ツールにレポートをエクスポートして、法的調査を行うこともできます。レポートは 10 日間利用できます。

保持

組織は、組織全体に適用される Webex Messaging および Webex Meetings のカスタムおよび別の保持期間を設定することで、リスクを管理し、グローバルな保持ポリシーに沿うことができます。Pro Pack for Control Hub により、フルアクセス権を持つ管理者は、組織の保持ポリシーと合わせて、その期間よりも古いデータを消去するための保持期間を設定できます。

管理者は組織全体のデータ保持ポリシーを定義して、関連するすべてのコンテンツが設定された保持期間に完全に削除されるようにすることができます。これにより、長期間での機密情報アクセスによるリスクが軽減され、さらに電子メールやその他のアプリケーションにおける保持ポリシーにも合わせることができます。

データ損失防止（DLP）

Webex には、2 重 DLP 戦略があります。まず、ユーザーが通信している環境を把握することです。ユーザーが通信しているコンテキストを認識させることで、データ損失の可能性について通知します。ユーザーには、特に、スペース所有権、適用される保持ポリシー、保持区分、外部参加者の有無に関する情報が通知されます。エンドユーザーは、

メッセージの削除、開封確認、スペースへのアクセス制御、モデレータ権限などの伝達制御機能によって強化されます。

この戦略の 2 番目の部分では、メッセージの投稿や削除、ファイルの添付、API を介してイベントとしてアクセスできる Webex のスペースへのユーザーの追加や削除などのユーザーアクションの監視が含まれます。これにより、DLP ソフトウェアを消費し、違反をチェックして修正できるようになります。コンプライアンス担当管理者は、ユーザーの行動を監視して対応するために、Webex Events API を使用して、イベントとコンテンツをポーリングできます。

Webex Messaging の他に、Webex Meetings 関連のイベントとメタデータおよびトランスクリプトも Events API を介して利用できます。パートナーの DLP エンジンは、API に対してクエリを実行し、会議、録音、トランスクリプトのリストを取得したり、アーティファクトをダウンロードして会議中の違反をスキャンしたりできます。さらに、コンプライアンス担当者は、議事録を編集したり、削除したりすることもできます。

リアルタイムファイル DLP の登場により、Webex DLP コンプライアンスの新たな利用方法論が誕生しました。リアルタイムファイル DLP を使用すると、DLP ベンダーは、ファイルが表示され、他のユーザーがダウンロードできるようになる前に、ファイルをスキャンして評価できます。これは、DLP アクションを、通常のオンプレミス インライン プロキシの動作と同様に、プロアクティブに検出/対処できるようになったことを意味します。今後数か月以内に、リアルタイム機能を他のユーザーのアクションに拡張する予定です。

DLP インテグレーションにアプローチするには、次の 3 つの方法があります。

- 既製ソリューション：インテグレーションは、主要なコンプライアンス パートナーによって認定されています。クラウド アクセス セキュリティ ブローカ（CASB）、DLP ISV、および Cisco CloudLock® は、Events API を介して Webex Messaging および Webex Meetings と統合され、Webex にターンキー DLP 機能を提供します。ポリシー違反をチェックし、是正するための措置を講じます。
- エンドツーエンドのカスタム ソリューション: お客様は、シスコ アドバンスド サービスと連携して、優先する DLP ベンダーとのカスタム インテグレーションを構築できます。
- 自己対応型：Webex Events API は公開されています。お客様は、API を使用して、自社のソリューションや他のサードパーティの DLP ベンダーと統合できます。

外部通信ブロック（BEC）：スペースメンバーシップ

組織間のコラボレーション（顧客、パートナー、ベンダーなどの別の組織に属するユーザとのコラボレーション）は、Webex Messaging の重要な機能であり、ワークフォースの生産性を向上させるうえで極めて重要です。ただし、組織間のコラボレーションでは、保護が必要な、データ損失や不正な通信の攻撃対象エリアも公開されます。ネイティブの外部通信ブロック（BEC）機能を使用することで、管理者は外部の組織や代理店との不正な通信を制御および防止できます。この機能により、管理者が承認したドメインに属する外部参加者とのみユーザの通信を許可するための、非常に要望の多い柔軟性が実現します。

Webex の管理者は、組織のユーザーがコラボレーションできるように、信頼できる許可された外部ドメインの許可リストを設定できます（現在は限定的に提供/トライアル中）。ユーザがスペースを作成し、組織が設定した許可リストに含まれるドメインに属していない外部組織から参加者を招待しようとした場合、招待された当該ユーザはスペ

ースに追加されません（メンバーシップ追加のアクションが失敗します）。ポリシーの決定はインラインで実行され、違反ユーザがスペースに追加される前にプロアクティブに適用されます。このように BEC ポリシーがインラインで実行され適用されることで、データ損失リスクが大幅に抑えられ、承認または信頼されていないドメインに属するユーザに対して公開されないよう組織が保護されます。

BEC ポリシーは常に、スペースを所有する組織を保護します。スペースに招待する外部ユーザは、スペースを所有する組織のドメイン許可リストに含まれるドメインに属している必要があります。スペースの所有者、招待者、招待されたユーザがそれぞれ異なる組織に属する組織間スペースでは、3 つの組織すべてのドメイン許可リスト ポリシーが評価され（BEC が有効な場合）、3 者のうち誰でもメンバーシップの追加を拒否できます。特定の状況では、管理者は非常に制限的なポリシーを必要とし、他の組織が所有するグループスペースへのユーザの参加を許可しない場合があります。管理者は、Control Hub で該当するトグルをオンにすることで、この追加の制限を簡単に適用できます。

BEC 設定は、1 対 1 のスペースやグループ スペースなど、さまざまなシナリオに適用されます。このポリシーは、ユーザが既存のスペースに追加されたとき、およびメンバーシップの追加を伴う新しいスペースの作成時に適用されます。

BEC ポリシーは、ポリシーが有効化された時点以降のスペースの新規作成アクティビティに対して適用され、既存のスペース（組織の BEC ポリシーが有効化される前に作成されたスペース）にさかのぼって適用されることはありません。管理者は、DLP パートナーを使用するか、カスタム スクリプトを作成して、既存のスペースで問題のあるユーザをスキャンして削除できます。

上記の組織全体のポリシー設定に加えて、管理者は特定の Active Directory（AD）グループのユーザーに適用する詳細なポリシーを作成することもできます。現在、AD グループのみがサポートする BEC ポリシーをサポートしています。組織管理者は、ディレクトリコネクタが有効になっていること（ディレクトリ コネクタ導入ガイド）と、ユーザーの AD グループ情報が組織の Active Directory サーバーから同期されていることを確認する必要があります。

この機能強化により、管理者は、組織のセキュリティ体制と外部コラボレーションルールに準拠しながら、選択した AD グループのユーザーに対してのみ外部コラボレーションを許可することができます。詳細な AD グループベースのアクセス許可は、許可/承認されたドメインの既存のリストに基づいて構築されます。つまり、選択した AD グループのユーザーは、承認されたドメインのリストにのみ属する外部ユーザーとコラボレーションできます。たとえば、管理者は、販売およびパートナーマーケティング組織のユーザーのみに、Webex Messaging を介して、承認されたドメインのリストに所属するユーザーと外部通信することを許可し、他のすべてのユーザー（銀行窓口、オペレーションなど）を内部通信のみに制限することができます。

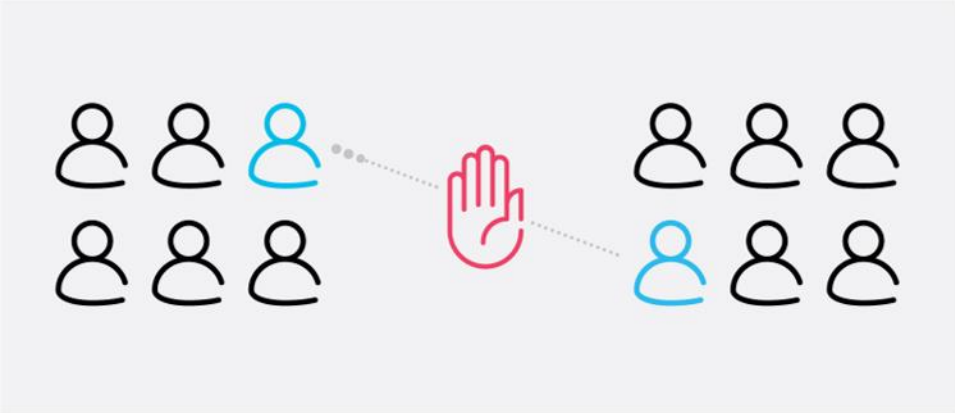
ポリシーの評価と施行はリアルタイムで行われます（遡及的な評価とポリシーの施行はサポートされていません）。

一括ドメイン追加ワークフローを使用すると、管理者はドメインのリスト（インポートごとに 500 のドメイン制限を持つ合計 2000 のドメイン）を作成し、それを Control Hub にインポートできます。このワークフローにより、管理者は、インポートファイル内のドメインのリストについて、未検証、未申請のドメイン、またはシンタックス（RegEx）エラーをチェックできます。管理者は、インポートを完了する前に未解決のエラーを修正できます。

これにより、組織の承認済みドメインのリストに多数のドメインを追加する必要がある管理者のセットアップ時間が大幅に短縮されます。

内部通信のブロック（BIC）：Ethical Wall

Ethical Wall（内部通信のブロックとも呼ばれます）を使用すると、管理者は Control Hub でルールを定義して、特定のユーザーグループが Webex スペースを介して相互にコラボレーションするのを防ぐことができます。管理者は、5 つの Active Directory グループごとに最大 5 つのポリシーを構成できます。ポリシーを定義すると対象のグループに所属するユーザは、お互いをスペースに招待できなくなるか、会話ができなくなりますが、社内の他のユーザーとは連絡を取り合うことができます。通常、ポリシーの施行はインラインで行われ、違反は発生前に特定およびブロックされます。



例えば、大手銀行では利益相反を避けるために、投資担当者と企業調査アナリストのコミュニケーションを制限する必要があります。Webex を使用すると、従業員は誰と通信できるかを心配する必要がなくなります。これは、Ethical Wall のポリシーにより、Control Hub で定義された単純なルールに基づいて制限されたユーザーの招待が自動的にブロックされるためです。

この機能により、組織は関連する会社の標準規格および規制（FINRA など）へのコンプライアンスを維持し、潜在的な利益相反を回避できます。

Ethical Wall 機能は、Control Hub で管理者がこの機能を有効化した後に先々の事を考えて機能します。今後の機能強化（現在は利用制限中）では、Webex スペース の既存の違反を遡及的にスキャンし、ポリシーに遵守していないスペースからユーザーを追い出し、違反を排除する機能を提供します。このシナリオは通常、ユーザーが転職したときや、AD グループ メンバーシップの変更の過程で発生します。このメンバーシップ変更により、1 つ以上の Ethical Wall ポリシー違反に該当する場合があります。

注：　上記の遡及的なポリシー適用のサポートは間もなく開始され、機能の一般提供時に利用可能になります（目標: 21 年第 4 四半期）。

統合の管理

Control Hub には、ユーザーによる統合への認定アクセスに関するポリシーを管理者が許可または拒否設定できる機能があります。この機能を使用して、developer.webex. com にある、API を使用して作成されたサードパーティアプリケーションを許可できるため、セキュリティおよびデータ処理の基準を満たすアプリケーションのみをユーザーに対して選択的に有効にすることができます。さらに、管理者は統合へのアクセスを取り消し、今後の承認を防ぐことができます。この機能には高度な機能が多く含まれています。詳細については、Webex ヘルプセンター をオンラインでご確認ください。

ボット管理：スペースメンバーシップ

管理者が Control Hub の設定を介してサードパーティの統合アプリに対する情報の流出を減らせる統合管理のように、ボットを管理するための追加機能があります。Control Hub の管理者は、組織のボットを許可または拒否するためのグローバル ポリシーを設定できます。「グローバル拒否」の場合は、個別のボットを許可できるため、組織の従業員が通信するためにグループとダイレクトのスペースでそれらのボットを利用できます。IT 管理者が知っておく必要があるのは、ボットを許可リストに登録するためのグローバルで一意な電子メール アドレスだけです。現時点では、ボット管理は既存のボット メンバーシップには適用されません（たとえば、すでにスペースに追加されていたボットは引き続き通信できます）。スペースの所有者、招待者、ボットがそれぞれ異なる組織に属している可能性がある混合スペースでは、3 つのエンティティすべてのポリシーが評価され、どの組織のポリシーでも当該のアクションが禁止されていない場合にのみボットが承認されます。

アーカイブ統合

お客様は、Webex のイベント API を使用して、アーカイブソフトウェアと統合できます。DLP と同様に、アーカイブ統合にアプローチするにはパートナーとすぐに使えるソリューション、パートナーまたはアドバンスドサービスが関与したエンドツーエンド カスタム ソリューションそして DIY ソリューションの 3 つの方法があります。

管理者アクティビティの監査

管理者アクションのログは、多くの組織および業界のコンプライアンス要件です。フルアクセス権を持つ管理者は、Control Hub に保存されている管理者監査ログを使用して、管理者によって実行された重要なアクション（組織設定の変更など）を表示できるようになり、REST API を介して露出できるようになりました。これらの管理者監査ログは、Control Hub で表示できます。ここで、特定の日付範囲内の管理者アクションを検索したり、特定のアクションまたは特定の管理者を検索したりできます。また、ログをカンマ区切り値（CSV）ファイルにエクスポートできます。

訴訟ホールド

訴訟ホールド機能により、コンプライアンス責任者の役割を持つユーザーは、組織の保持ポリシーに関係なく、訴訟が合理的に予想される場合に、ユーザーに関連付けられた関係するすべての形式の関連コンテンツを保持できます。コンプライアンス責任者は、法的事項を作成したり、管理者（ユーザー）を訴訟ホールドにしたり、問題を表示、ダ

ウンロード、およびリリースしたりできます。訴訟ホールド中のデータは、組織の保持期間に基づいて削除の対象となることはありません。ケースがクローズされると、訴訟ホールドを解除でき、その時点でそのデータは組織の保持期間に基づいて削除の対象になります。

Webex コンテンツの訴訟ホールドは、Webex Spaces に投稿されたメッセージ、ファイル、ホワイトボード、その他のコンテンツをサポートします。さらに、録音、トランスクリプト、ハイライトなどの Webex Meetings コンテンツもサポートします。

エンタープライズ コンテンツ管理の統合

ネイティブのファイル共有とストレージに加えて、Webex は IT 管理者がユーザーに対して Microsoft OneDrive、SharePoint Online、および Box をエンタープライズ コンテンツ管理（ECM）ソリューションとして有効にできる柔軟性も備えています。ユーザーは Webex スペースで直接、OneDrive、SharePoint Online、Box の最新のファイルを共有、編集（BOX では非対応）、取得できます。

これは、 Control Hub で 1 回切り替えるだけでセットアップできます。また、既存のファイル共有権限およびデータ損失防止（DLP）ポリシーを変更する必要はありません。IT 管理者には、有効にする SharePoint Online および OneDrive のドメイン、または Microsoft Azure のテナント ID を決定する完全な権限があります。これにより、IT によって承認されたドメインのみが利用可能になり、ユーザーは個人の OneDrive フォルダーを使用できないため、データ損失のリスクがなくなり、同時にマルウェアの脅威から保護されます。

最高レベルの管理の場合、IT 管理者はすべてのコンテンツが既存のエンタープライズ ファイル ストレージ サービスを通じてルーティングされるように、Webex でネイティブ ファイル ストレージをオフにすることもできます。新しいファイルとフォルダは、Webex から OneDrive、SharePoint Online、Box にアップロードできます。また、Webex 内でファイルの共有、表示、共同編集（Box では非対応）も可能です。

ユーザが Microsoft OneDrive または SharePoint Online のフォルダ内のファイルで共同作業するときは、スペースをそのフォルダにリンクできます。ユーザーは、Webex スペースから直接、リンクされたフォルダ内のファイルにアクセスし、（Control Hub の設定に基づいて）スペースのデフォルトストレージとして設定することができます。この場合、そのスペースで共有されるすべてのファイル（スクリーンキャプチャを含む）が、Webex のネイティブストレージではなく、リンクされた ECM フォルダに保存されます。

Webex ECM 統合ソリューション：

- IT 管理者は、ファイル共有とストレージ用に、Webex のネイティブ ファイル ストレージか、Microsoft OneDrive、SharePoint Online、Box および Google Drive のどちらかを有効にすることができます
- IT 管理者は、Microsoft OneDrive および SharePoint Online との統合のためのデフォルト ストレージ オプションを使用して、フォルダをスペースにリンクすることができます。
- ユーザは、Webex Team スペースで ECM システムからファイルを共有、オープン、編集、共同編集することができます
- スペースメンバーは、Webex スペースからファイルやフォルダを ECM システムにアップロードすることができます

- ユーザーは、Microsoft OneDrive および SharePoint Online の共有ファイルを確認して共同編集できる人を定義できます
- ユーザーが常に最新バージョンのファイルを表示できるようにします
- ECM ファイル、メッセージ、およびホワイトボード図面へのリンクをエンドツーエンドで暗号化します
- 既存の DLP と連携動作すると、Webex スペースで共有されているファイルの追加のコピーが作成されません
- 個人用またはシャドー IT の OneDrive または SharePoint Online のフォルダをブロックし、承認されたインスタンスのみ許可します

コンプライアンス機能の概要

表 3 に、Webex のコンプライアンス機能の概要を示します。

表 3. コンプライアンス機能

機能	説明
eDiscovery レポート：電子メールベースおよびスペースベースの検索	コンプライアンス管理者は、ユーザーの電子メールアドレスまたはスペース名を使用して、コンテンツのメッセージと会議を検索および抽出できます。現在のユーザと削除されたユーザの両方について、複数のカンマ区切りの電子メール アドレスを入力として使用できます。電子メールアドレス数のハードリミットは 500 で、数 GB の範囲の大規模なレポートを生成できます。
eDiscovery レポート：時間枠	コンプライアンス管理者は、検索する期間を定義できます。 **標準オファー：**過去 90 日間以内に生成されたデータを検索可能。 **Pro Pack：**過去 90 日間より前に生成されたデータも検索可能。
eDiscovery レポートのダウンロード	コンプライアンス管理者は、過去のレポートのリストを表示し、ダウンロードできます。その後、選択した eDiscovery ツールにレポートをインポートして、法的調査を行うことができます。オプションで、ダウンロードから添付ファイルを除外してメッセージのみを検査し、対象のスペースまたはユーザを特定することもできます。レポートは 10 日間利用できます。数 GB の範囲の大規模なレポートを生成してダウンロードできます。
保持	**標準オファー：**メッセージングの無期限の保存と設定不可。 **Pro Pack：**管理者は、Webex Messaging および Webex Meetings でのデータの保持期間を設定できます。この期間を過ぎると、すべての Webex Messaging コンテンツ（ファイル、メッセージ、およびイベント）と Webex Meetings コンテンツ（録画、議事録、およびハイライト）が消去され、アクセスできなくなります。保持期間は、Webex 内のすべてのスペースに適用されます。Webex Meetings の保持ポリシーは、すべての会議の録音、トランスクリプト、およびハイライトに適用されます。
訴訟ホールド	**標準オファー：**利用できません。 **Pro Pack：**組織内のコンプライアンス責任者の役割を持つユーザーは、組織の保持ポリシーに関係なく、電子証拠の開示の必要性が予想される場合に、ユーザに関連付けられた関係するすべての形式の関連コンテンツを保持できます。コンプライアンス責任者は、法的事項を作成したり、管理者（ユーザー）を訴訟ホールドにしたり、問題を表示、ダウンロード、およびリリースしたりできます。訴訟ホールドは、Webex Messaging と Webex Meetings のコンテンツをサポートします
Webex Events API：DLP	Webex イベント REST API は DLP ソフトウェアと統合することで、ポリシー違反をチェックし、問題を修復するための措置を講じることができます。利用可能なユーザ

機能	説明
	ーアクションには、メッセージやファイルの投稿、スペースへのユーザの追加、完了した会議、議事録が含まれます。実行されるアクションとして、DLP ポリシーが定義したユーザーや管理者への警告、メッセージの削除（メッセージのみ）、アラームの設定などが挙げられます。 **標準オファー：**リアルタイム イベント API アクセス。カスタム データ範囲は過去 90 日以内である必要があります。 **Pro Pack：**リアルタイム イベント API アクセス。データの保持期間内のカスタムデータ範囲が設定され、利用可能になります。
Webex Events API：アーカイブの統合	アーカイブ ソフトウェアで Webex Events API を使用して、Webex Messaging および Webex Meetings のデータをアーカイブすることができます。 **標準オファー：**リアルタイム イベント API アクセス。カスタム データ範囲は過去 90 日以内である必要があります。 **Pro Pack：**リアルタイム イベント API アクセス。カスタム データ範囲に制限はありません。
エンタープライズ コンテンツ管理の統合	また、Webex は、独自のネイティブ ファイル共有とストレージに加えて、Microsoft OneDrive、SharePoint Online、Box、Google Drive をエンタープライズコンテンツ管理（ECM）ソリューションとして使用できるように IT 管理者が設定できる柔軟性も備えています。その結果、ユーザーは Webex スペース 内で直接、OneDrive ファイルおよび SharePoint Online の最新のファイルを共有、編集（Box では未対応）、取得できます。OneDrive および SharePoint Online のフォルダをスペースにリンクして、コンテンツを一括で共有することもできます。さらに、それらのフォルダをスペースのデフォルト ストレージにすることもできます。 **標準オファー：**Microsoft OneDrive と SharePoint Online、Box と Google Drive の統合。ただし、Webex ネイティブ ファイル ストレージを無効にする機能はありません。 **Pro Pack：**Webex ネイティブ ファイル ストレージを無効にする機能がある Microsoft OneDrive と SharePoint Online、Box と Google Drive の統合。
外部通信のブロック（BEC）	管理者は、（異なる組織のユーザーとのスペース メンバーシップを許可することで）組織間のコラボレーションを可能にし、Webex の機能をフル活用しながら、信頼できないドメインに対して組織とユーザが公開されないよう保護することができます。管理者は、承認済みドメインの許可リストを簡単に作成して、信頼できるドメインからの参加者とのみユーザーが通信できるように設定することができます。管理者は、最大 **2000** 個のドメインを許可リストに含めることができます。一括ドメイン追加ワークフローを使用すると、管理者はアップロードごとに 1 つの csv ファイルを介して最大 500 のドメインを追加できます。これにより、ドメインを個別に追加する面倒なタスクが軽減されます。インラインでのポリシーの適用により（組織の許可リストに含まれるドメインに属しているユーザであることが確認された後にのみスペースへのユーザの追加が許可されます）、信頼できないドメインやデータ漏洩にユーザがさらされるリスクを最小限に抑えます。さらに、管理者は、特定の AD からのユーザーに選択的に外部通信を許可することもできます。 **標準オファー：**BEC は標準オファーには含まれていません。 **Pro Pack：**最大 2000 ドメインをサポートするフル機能。
内部コミュニケーションのブロック（BIC）- Ethical Wall	IT 管理者は、組織内の特定のユーザーグループ間における連絡の取り合いを防ぐことができます。これは、組織が関連する業界標準規格および規制（FINRA など）への遵守を維持し、潜在的な利益相反を回避するのに役立ちます。 **標準オファー：**なし **Pro Pack：**インラインポリシーチェックの完全な機能。

機能	説明
ボット管理	管理者は、ボット管理ポリシーを設定して、ボットを全体的に許可または拒否することができます。全体的に拒否する場合、ボットの一意の電子メールアドレスを使用して個別のボットを選択的に許可できます。異なる組織のメンバーが参加する混合スペースは、スペースの所有者、招待者、および招待された組織（ボット）が関係するため、制限が最も厳しいポリシーに基づいて評価されます。 **標準オファー：**ボット管理の全体的な許可または拒否。 **Pro Pack：**グローバル フラグが拒否に設定された、個別のボットの許可リスト。
統合の管理	**標準オファー：**管理者は、すべての統合に対するユーザのアクセスを有効または無効にできます。 **Pro Pack：**管理者は、すべてのユーザーまたは特定のユーザーセットに対する特定の統合の有効化または無効化、ユーザーによる統合の導入の監視、統合のアクセスの取り消し、統合をアクティブに使用しているユーザーの電子メールアドレスのリストのダウンロードを行えます。 組織に対して統合が無効化されている場合、ユーザーは、スペースに統合を追加することを承認し、ユーザーの代理として行動することはできません。

よくある質問

Q. コンプライアンス責任者として、自社が所有していないスペースで自社の従業員が投稿したコンテンツを検索できますか。

A. はい。コンプライアンス責任者は、従業員が所属するすべてのスペースで、組織の従業員によって投稿されたコンテンツを検索できます。

Q. コンプライアンス責任者として、会社の従業員が主催する会議のトランスクリプトと録音を検索できますか。

A. はい。コンプライアンス責任者は、組織の会議サイトで、組織の従業員が主催する会議のトランスクリプトと録音を検索できます。

Q. コンプライアンス責任者として、外部組織の会議サイトで主催された会議のトランスクリプトと録音を検索できますか。

A. いいえ。コンプライアンス責任者は、外部組織の会議サイトで主催された会議のトランスクリプトと録音を検索できません。

Q. お客様が、Webex で統合が認定されていない CASB またはアーカイブ システムを導入した場合はどうなりますか。

A. その場合は、以下の 2 つの追加オプションがあります。

Events API を使用して、Webex と CASB またはアーカイブ システム間の統合を構築します

Cisco アドバンスド サービスと連携して、Events API を使用して統合を構築します

Q. Events API を通じて公開されるイベントのタイプにはどのようなものがありますか。

A. Events API は次のイベントをキャプチャします。

- メッセージの投稿
- ファイルの投稿
- ファイルのダウンロード
- メッセージまたはファイルの削除
- スペースへのユーザの追加
- スペースからのユーザの削除
- ホワイトボードのスナップショット
- 会議イベント
- トランスクリプト イベント

シスコの環境維持への取り組み

Cisco 製品、ソリューション、運用および拡張運用またはサプライチェーンに対する環境持続可用性ポリシーと取り組みに関する情報は、Cisco の企業の社会的責任（CSR）レポートの「環境持続可用性」項を参照してください。

次の表に、環境の持続性に関する主要なトピック（CSR レポートの「環境の持続性」セクションに記載）への参照リンクを示します。

持続可能性に関するトピック	参照先
製品の材料に関する法律および規制に関する情報	材料
製品、バッテリ、パッケージを含む電子廃棄物法規制に関する情報	WEEE 適合性

シスコでは、パッケージデータを情報共有目的でのみ提供しています。これらの情報は最新の法規制を反映していない可能性があります。シスコは、情報が完全、正確、または最新のものであることを表明、保証、または確約しません。これらの情報は予告なしに変更されることがあります。

Cisco Capital

目的達成に役立つ柔軟な支払いソリューション

Cisco Capital により、目標を達成するための適切なテクノロジーを簡単に取得し、ビジネス変革を実現し、競争力を維持できます。総所有コスト（TCO）の削減、資金の節約、成長の促進に役立ちます。シスコの柔軟な支払いソリューションは 100 か国以上で利用可能であり、ハードウェア、ソフトウェア、サービス、およびサードパーティ製の補完的な機器を、利用しやすい計画的な支払方法で購入できます。詳細はこちらをご覧ください。

免責事項：データ損失防止（DLP）、eDiscovery、データ保持、訴訟ホールドなどの Webex Meetings 向けコンプライアンス機能は、2020 年 9 月から利用できます。

米国本社
Cisco Systems, Inc.
サンノゼ(カリフォルニア州)

アジア太平洋本社
Cisco Systems (USA) Pte. Ltd.
シンガポール

ヨーロッパ本社
Cisco Systems International BV Amsterdam,
アムステルダム(オランダ)

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト(https://www.cisco.com/go/offices [英語])をご覧ください。

Printed in USA C78-740772-05 01/22